UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/739,260	12/19/2000	Ravi Sandhu	3001-07	5789

20457 7590 04/18/2005

ANTONELLI, TERRY, STOUT & KRAUS, LLP
1300 NORTH SEVENTEENTH STREET
SUITE 1800
ARLINGTON, VA 22209-3873

EXAMINER	
DAVIS, ZACHARY A	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 04/18/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/739,260	SANDHU ET AL.	
	Examiner	Art Unit	
	Zachary A Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 January 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-10,12-18 and 20-26* is/are rejected.

7)☒ Claim(s) *2,11,19 and 27-31* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. An amendment was received on 14 January 2005. Claim 14 has been amended. No claims have been added or canceled. Claims 1-31 are currently pending in the present application.

Response to Arguments

2. Applicant's arguments filed 12 October 2004 have been fully considered but they are not persuasive.

Claims 17 and 26 were rejected under 35 U.S.C. 102(b) as being anticipated by Ganesan, US Patent 5535276. Claims 1-16, 18-25, and 27-31 were rejected under 35 U.S.C. 103(a) as being unpatentable over Ganesan in view of Spies et al, US Patent 6230269.

In reference to Claims 17 and 26, Applicant argues that Ganesan does not disclose transformation of a message with a user generated first key portion. The Examiner respectfully disagrees. Applicant concedes that Ganesan discloses that a temporary public key portion, which the Examiner believes corresponds to the claimed first message, is encrypted (or transformed) with the first private key portion of the permanent key to form a first message, which the Examiner believes corresponds to the claimed second message (see also column 8, lines 24-28). It is also noted that the first private key portion of the permanent key is indeed generated by the user (see column

14, lines 29-32). Applicant further argues that the limitation that the first private key portion not be stored at a networked device or transmitted over a network has not been addressed. However, the Examiner believes that Ganesan does disclose such a limitation; for example, Ganesan discloses that the first private key portion is known only to the user (column 15, lines 22-26) and that the first portion is not communicated to any other users or devices in any form other than when it has been used as an encryption key (see column 16, lines 30-41).

In reference to Claim 1, Applicant argues that Ganesan does not disclose two processors. However, the Examiner believes that Ganesan does indeed disclose, *inter alia*, a first processor, which generates an asymmetric key pair, divides the key into two parts, where one of the parts is a user password, and stores only the second private key portion and public key in a persistent state (see column 15, lines 22-26, where the authentication server 120 and the ticket granting server 140 comprise the first processor); and a second processor representing a user which generates a first private key portion (column 15, lines 9-11, where processor 110 corresponds to the second processor; column 14, lines 29-32, where the user portion of the private key is the user password; and column 15, lines 39-60, where the first processor generates and uses the user portion of the long term private key). Applicant further argues that Ganesan does not teach destruction of the keys; however, the Examiner believes that the cited portion of Ganesan, column 14, line 66-column 15, line 2, does indeed disclose destruction of key information. Specifically, at column 14, lines 55-66, Ganesan discloses that the first private key portion is known only to the user, the second portion

is stored in a secure database, and the public keys are known; the Examiner believes that in this context, the phrase "All other intermediate key generation information has been destroyed" refers to all other key information, including the full private key.

In reference to Claim 18, Applicant argues that Ganesan does not disclose a separate generation of only the first private key portion; however, the Examiner believes that Ganesan discloses, *inter alia*, that the first private key portion is a password generated by the user (column 14, lines 29-32) and the user is represented by a separate processor (column 15, lines 9-15, where processor 110 represents the user).

In reference to Claim 9, Applicant similarly argues that Ganesan does not disclose transforming a message with a generated first portion of a private key, but that Ganesan instead discloses generation of a temporary key which is encrypted with a portion of a permanent key. However, as stated above, the Examiner believes that the temporary key, which is encrypted by the first portion of the permanent public key, corresponds to the message that is transformed as claimed by Applicant.

Regarding Claims 1, 9, and 18, in response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Specifically, Applicant concedes that Spies does teach the use of passwords in generating keys; however, Applicant argues that Spies does not teach or suggest division of a private key based on a password or generation of a first portion of a private key based on a password. The Examiner notes that Spies was

not relied upon to teach division of a key based on a password; instead, Ganesan teaches such a division of a key based on a password (column 14, lines 30-34). Thus, the Examiner believes that the combination of the division of a key and the generation of a key using a password, as taught by Ganesan and Spies, fairly suggests the division of a key based on a password as claimed by Applicant.

In reference to Claims 2, 11, 19, and 27, Applicant argues that the prior art does not teach or suggest that the user password has a bit length between 56 and 72 bits nor that the first portion of the private key have a bit length of at least 257 bits. Regarding the first limitation, the Examiner believes that the cited portion of Ganesan, column 3, lines 31-40, states that a password can be, for example, 8 to 12 characters long; it is noted that, for example, the ASCII representation of a character is 7 bits long, and therefore, 8 characters at 7 bits per character would be a password of 56 bits. Regarding the second limitation, however, the Examiner finds Applicant's argument persuasive, and this matter is addressed below.

In reference to Claims 4, 13, 21, and 29, Applicant argues that the prior art does not teach or suggest selectively operating in one of two modes; however, Applicant concedes that Spies does disclose multiple implementations, and the Examiner believes that these multiple implementations imply that one of them must be selected for use.

In reference to Claims 5, 7, 14, 16, 22, 23, 30, and 31, Applicant argues that Spies does not disclose, as previously asserted by the Examiner, that the strength of the user password in relied on in the generation of keys. The Examiner disagrees, and

believes that the cited portion of Spies, column 8, lines 19-21, does disclose this; it is further noted that the entropy of the password is an indication of its strength.

In reference to Claims 6 and 15, Applicant argues that Spies does not disclose selection of a one way function from a group of one way functions; however, Applicant concedes that Spies does disclose a group of one way functions, and the Examiner believes that the presence of such a group implies that one of these functions must be selected for use.

The arguments regarding Claims 8 and 24, regarding transformation of a message with a first private key portion have been addressed above, for example in reference to Claims 17, 26, 1, and 9.

Therefore, for the reasons above, the Examiner maintains the rejections detailed below.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 17 and 26 are rejected under 35 U.S.C. 102(b) as being anticipated by Ganesan, US Patent 5535276.

In reference to Claim 17, Ganesan discloses a system including a first networked device representing a user that generates a first private key portion, transforms a message with the first portion to form a second message (where the first message is the temporary key portion and the second message is the first encrypted message formed at column 8, lines 24-27; see also column 15, lines 52-54), and transmits the second message (column 8, lines 24-32). Ganesan also discloses a second networked device that stores a public key and a second private key portion (column 14, lines 59-66), receives the second message (column 8, lines 24-32), and further transforms the second message with the second private portion (column 8, lines 28-32; see also column 15, lines 61-63). Ganesan further discloses that the first private key portion is not stored at any networked device and not transmitted over the network (noting column 14, lines 55-56, where the first private key portion is known only to the user).

In reference to Claim 26, Ganesan discloses a method including generating a first private key portion, transforming a message with the first portion (column 8, lines 24-27), and further transforming the first message with the second private key portion (column 8, lines 28-32). Ganesan further discloses that the first private key portion is not stored at any networked device and not transmitted over the network (noting column 14, lines 55-56, where the first private key portion is known only to the user).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1, 3-10, 12-16, 18, and 20-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ganesan in view of Spies et al, US Patent 6230269.

In reference to Claim 1, Ganesan discloses a system including a first processor (see column 15, lines 22-26, where the authentication server 120 and the ticket granting server 140 comprise the first processor) that generates a private key and public key pair (column 14, lines 29-30); divides the private key into a first portion, which is a user's password, and a second portion (column 14, lines 30-34); destroys the private key and the first portion (column 14, line 66-column 15, line 2, noting that, because in column 14, lines 55-66, the first private portion is known only to the user and the second portion and public key are stored, whereas all other key information is destroyed, this necessarily refers to the full private key); and stores the second portion and the public key (column 14, lines 59-66). Ganesan also discloses a second processor representing the user (column 15, lines 9-11, where processor 110 corresponds to the second processor) that generates the first private key portion upon input of the user's password (column 14, lines 30-32) and then destroys the first portion (column 14, line 66-column 15, line 2; column 19, lines 27-29; also noting column 14, lines 55-56 where the first

portion is known only to the user). However, although Ganesan discloses that the first private key portion is a user's password, Ganesan does not explicitly disclose that the first portion is generated based on the user's password.

Spies discloses an authentication system in which a key is formed from a user's password (column 7, lines 36-41). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Ganesan by generating the first private key portion based on the user's password, instead of using the password itself as the first portion, in order to allow users the increased flexibility and convenience of generating keys at any computer on a network using only a password (see Spies, column 2, lines 45-48).

In reference to Claim 3, Spies further discloses generating the first portion using a one way function (column 5, lines 35-37; column 7, lines 36-41).

In reference to Claim 4, Spies further discloses that the processors can operate in two modes (column 7, lines 36-47; column 8, lines 17-24) and that the one way function can be applied a varying number of times (column 5, lines 35-37).

In reference to Claims 5 and 7, Spies further discloses relying on the strength of the user password in generating keys (column 8, lines 19-21).

In reference to Claim 6, Spies further discloses selecting the one way function from a group of one way functions (column 5, lines 42-46).

In reference to Claim 8, Ganesan further discloses that the second processor encrypts a message with the first private key portion (column 8, lines 24-27) and that

the first processor recovers the message using the second private key portion and the public key (column 8, lines 28-32).

In reference to Claim 9, Ganesan discloses a system including a first processor representing a user that generates a first private key portion, which is a user's password (column 14, lines 30-32); transforms a message using the first portion (column 8, lines 24-27); and destroys the first portion (column 14, line 66-column 15, line 2; column 19, lines 27-29). Ganesan also discloses a second processor that further transforms the transformed message by applying a second private key portion and a public key corresponding to the first portion (column 8, lines 28-32). However, although Ganesan discloses that the first private key portion is a user's password, Ganesan does not explicitly disclose that the first portion is generated based on the user's password.

Spies discloses an authentication system in which a key is formed from a user's password (column 7, lines 36-41). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Ganesan by generating the first private key portion based on the user's password, instead of using the password itself as the first portion, in order to allow users the increased flexibility and convenience of generating keys at any computer on a network using only a password (see Spies, column 2, lines 45-48).

In reference to Claim 10, Ganesan further discloses a storage device storing the second portion and the public key, that the second processor retrieves the stored

second portion and public key, and that the first portion is never stored in a persistent state (column 14, line 59-column 15, line 2).

In reference to Claim 12, Spies further discloses generating the first portion using a one way function (column 5, lines 35-37; column 7, lines 36-41).

In reference to Claim 13, Spies further discloses that the processors can operate in two modes (column 7, lines 36-47; column 8, lines 17-24) and that the one way function can be applied a varying number of times (column 5, lines 35-37).

In reference to Claims 14 and 16, Spies further discloses relying on the strength of the user password in generating keys (column 8, lines 19-21).

In reference to Claim 15, Spies further discloses selecting the one way function from a group of one way functions (column 5, lines 42-46).

In reference to Claim 18, Ganesan discloses a method including generating a private key and a public key (column 14, lines 29-30), dividing the private key into a first portion and a second portion (column 14, lines 30-34), destroying the private key and the first portion without storage (column 14, line 66-column 15, line 2), generating the first portion (column 14, lines 30-32), and destroying the first portion without storage (column 14, line 66-column 15, line 2; column 19, lines 27-29). However, although Ganesan discloses that the first private key portion is a user's password, Ganesan does not explicitly disclose that the private key and the first portion are generated based on the user's password.

Spies discloses an authentication system in which a key is formed from a user's password (column 7, lines 36-41). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Ganesan by generating the first private key portion based on the user's password, instead of using the password itself as the first portion, in order to allow users the increased flexibility and convenience of generating keys at any computer on a network using only a password (see Spies, column 2, lines 45-48).

In reference to Claim 20, Spies further discloses generating the first portion using a one way function (column 5, lines 35-37; column 7, lines 36-41).

In reference to Claim 21, Spies further discloses that the processors can operate in two modes (column 7, lines 36-47; column 8, lines 17-24) and that the one way function can be applied a varying number of times (column 5, lines 35-37).

In reference to Claim 22, Spies further discloses relying on the strength of the user password in generating keys (column 8, lines 19-21).

In reference to Claim 23, Spies further discloses selecting the one way function from a group of one way functions (column 5, lines 42-46) and relying on the strength of the user password in generating keys (column 8, lines 19-21).

In reference to Claim 24, Ganesan further discloses transforming a message with the first portion (column 8, lines 24-27) and further transforming the message using the second portion and the public key (column 8, lines 28-32).

In reference to Claim 25, Ganesan further discloses storing and retrieving the second portion and the public key and that the first portion is never stored in a persistent state (column 14, line 59-column 15, line 2).

Allowable Subject Matter

7. Claims 2, 11, 19, and 27-31 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

8. The following is a statement of reasons for the indication of allowable subject matter: Claims 2, 11, 19, and 27 are dependent on rejected claims 1, 9, 18, and 26, respectively. The cited prior art, Ganesan and Spies, disclose everything as applied to the independent claims, as described above. Ganesan further discloses that the password used has a bit length of 56-72 bits (column 3, lines 31-40, as discussed above). However, neither Ganesan nor Spies, alone or in combination, teach or suggest the specific limitation that the generated first private key portion has a bit length of at least 257 bits. Claims 28-31 have been indicated as allowable subject matter due to their dependence on Claims 27.

Conclusion

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

zad

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER